Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF THE DIVISION OF BANKING SUPERVISION AND REGULATION'S DISTRIBUTED PROCESSING ENVIRONMENT

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

July 1, 1997

Mr. Richard Spillenkothen, Director
Division of Banking Supervision and Regulation

We are pleased to present our final *Report on the Audit of the Division of Banking Supervision and Regulation's Distributed Processing Environment* (A9610). We performed this audit to determine if the Division of Banking Supervision and Regulation (BS&R) has established an effective process for planning, organizing, directing, and controlling the activities related to distributed processing; is adequately managing its local area networks and has developed an effective problem management system; properly secured its distributed systems and data; and developed appropriate backup and disaster recovery procedures.

Overall, we found that BS&R is adequately managing its distributed processing environment. BS&R's *Strategic Office Automation Plan*, which covers the 1995 through 1997 time frame, identified major objectives which were consistent with Systemwide initiatives and helped maintain a high level of system performance. BS&R has also taken steps to develop appropriate back-up and disaster recovery procedures, and to build an effective problem management system for users.

Notwithstanding these accomplishments, we are concerned that organizational issues will impact BS&R's ability to effectively and efficiently meet distributed processing challenges that are and will be facing the division and the Systemwide supervision and regulation function. While security over BS&R's network is generally adequate, controls could be strengthened by implementing additional security features. With BS&R moving forward to a dual network operating system and a new office application suite this year, it will be particularly important to examine security capabilities and controls. We found nine vulnerabilities that indicate controls need to be enhanced in the division's use of the Novell NetWare operating system and provided these technical findings, along with specific recommendations for corrective action, under a separate restricted cover to the Deputy Director of BS&R for appropriate disposition. Finally, we believe opportunities exist to improve communications and strengthen network management and control by formalizing policies and procedures and by ensuring that problems are consistently resolved in a complete and timely manner. This report contains five recommendations designed to help you guide the division's distributed processing environment as you move forward.

We provided a draft of this report for you and your staff's review and comment. Your response indicates agreement with all of our recommendations.

A copy of this report is being sent to members of the Board's Committee on Bank Supervision and Regulatory Affairs, the Vice Chair as Administrative Governor, and selected Board staff. The report is available to the public, and a summary will appear in our next

semiannual report to Congress. We plan to follow-up on implementation of our recommendations and will report any exceptions as part of our future audit activities.

Sincerely,

Barry R. Snyder
Assistant Inspector General for Audits

Enclosure

Board of Governors of the Federal Reserve System

REPORT ON THE AUDIT OF
THE DIVISION OF BANKING
SUPERVISION AND REGULATION'S
DISTRIBUTED PROCESSING
ENVIRONMENT

OFFICE OF INSPECTOR GENERAL

TABLE OF CONTENTS

BACKGROUND

Overview

Over the past several years, the Board of Governors of the Federal Reserve System (the Board) has shifted its resources to provide analytical tools to users at their desktops while reserving large-scale processing and storage functions for the mainframe and larger distributed servers. The desktop computing environment offers users a powerful, cost-effective set of tools for handling data. Although desktop computing gives users convenient access to data and greater control over information, operational management functions such as security, backup and recovery, and production processing are generally more fully developed in the mainframe counterparts. Acquiring a network system is simply the first step in implementing and maintaining a distributed processing environment. Operational functions such as training, problem resolution, tuning, configuration management, and planning must also be performed. Control weaknesses in these operational functions can be overcome by establishing an effective process for planning, organizing, directing, and controlling the activities related to distributed office automation systems; managing the efficiency of the local area networks (LANs); developing an effective problem management system; properly securing the system and data; and developing appropriate backup and disaster recovery procedures.[1]

To protect its information assets from loss or misuse, the Federal Reserve System (the System) recently issued the *Information Security Manual* (*ISM*), which defines the security policies and safeguards for information security. The *ISM* is applicable to all automated platforms and manual processes used throughout the System.[2] Two other manuals, the *Distributed Processing Information Security Support Manual,* and the *Mainframe and FEDNET Information Security Support Manual*, discuss policies and procedures specifically related to those data processing environments. Board divisions and offices were expected to comply with the policies and safeguards in these manuals as of January 1, 1997.

The Banking Supervision and Regulation Function

A major responsibility of the System is to foster a strong, stable, responsive, and competitive banking and financial system. Through its supervision and regulation (S&R) function, the System

---

[1]A local area network (LAN) is a group of computers and other devices that are connected to exchange information and are typically dispersed throughout a small area, such as a building or office. A LAN can be connected to a larger network.

[2]The "System" is used throughout the report to refer to the Board and the Federal Reserve Banks.

also works to ensure that financial institutions operate in a safe and sound manner and in compliance with applicable laws and regulations.[3]

By statute, the Board is responsible for carrying out the System's supervision and regulation of financial institutions and has delegated S&R functions to its Division of Banking Supervision and Regulation (BS&R) and the Federal Reserve Banks. BS&R directs and coordinates the supervisory work of the Reserve Banks and reviews actions that the Reserve Banks take under delegated authority. BS&R also disseminates the supervisory and regulatory policies and procedures of the Board. Within this framework, each Reserve Bank has a high level of autonomy in organizing its S&R operations, in designing business processes to meet Board mandates, and in applying resources—including information technology resources—to meet its S&R needs.

The S&R Function's Distributed Processing Environment

The S&R function depends on vast amounts of information to carry out its mission effectively, and has long been committed to using information technology to manage this information. Over the years, the S&R function has developed numerous, diverse distributed processing systems, many of them tailored to individual Reserve Banks. Though the autonomy of each Reserve Bank has made it difficult to build information technology solutions that are adopted Systemwide, the S&R function recognized the potential benefits of managing and delivering information on a common basis across the System and is taking steps to increase commonality.

To encourage Systemwide involvement in the technological decision-making process, BS&R works closely with the officers in charge of supervision from the Reserve Banks; chairs the Banking Supervision and Regulation Strategic Planning Steering Committee, which helps administer and coordinate implementation of the Federal Reserve's S&R strategic plan; and participates in the Information Technology Committee (ITC), a subgroup of the Strategic Planning Steering Committee that coordinates the acquisition and use of automation, communication, and information management technology within the S&R function. Committees and working groups have historically played a key role in S&R information technology development. In the 1990s, for example, the Automation Oversight Committee (which preceded the ITC) supported development of the Federal Reserve Examination Data (FRED) system, a client–server application designed to serve as a central repository for System supervisory data.

Recently, the S&R function took a big step toward standardizing its distributed processing environment, which currently consists of local and remote workstations using a variety of operating systems and desktop tools. In June 1996, based on the ITC's recommendation, the officers in charge of supervision approved two software standards for Systemwide implementation. On July 12, 1996, the Director of BS&R issued Administrative Directive (AD) 96-39, which

---

[3]The "S&R function" is used throughout the report to refer to the supervision and regulation function of the Federal Reserve System, which includes the Reserve Banks and the Board.

states that, effective July 1, 1997, the supervision function's PC operating system standard will be Microsoft's Windows 95 for portable PCS and Windows New Technology (Windows NT) for desktop systems. AD 96-39 further states that, effective January 1, 1998, the supervision function's software application standard will be Microsoft Office. The AD also outlines minimum and recommended hardware configurations. BS&R and the Reserve Banks are both expected to convert to these software standards within the specified time frames.
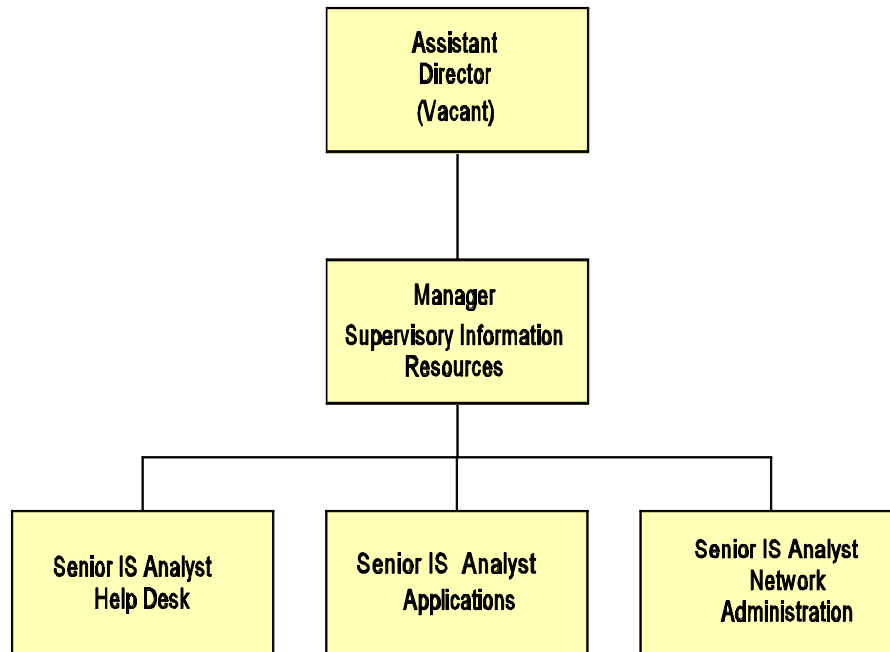

BS&R's Supervisory Information Resources Section

The Supervisory Information Resources (SIR) section within the BS&R was created in 1986 to provide direction to the division's automation program. SIR currently has an operating budget of $1.15 million, with eleven budgeted positions (see figure 1 for the SIR organization chart). A major objective of SIR is to manage the operation and growth of divisionwide office automation systems. SIR implements and manages the divisions's network at multiple sites, prepares the division's *Strategic Office Automation Plan*, develops divisionwide information systems, installs hardware and software, maintains the division's data security program, and assists division personnel in using distributed office automation systems. SIR also serves as a liaison with the Division of Information Resource Management (IRM) on BS&R office automation and data processing requirements, application development, planning and implementation. Additionally, SIR provides management guidance and technical support for the division's automation initiatives and acts as a resource for division information needs by budgeting and managing office automation acquisitions and installations and by coordinating the division's IRM budget. Finally, SIR had historically represented BS&R in System committees dealing with data processing and office automation matters affecting the division, although a vacancy at the assistant director level (see figure 1) has since limited its participation.

BS&R's office automation began in 1984 with the acquisition of four stand-alone IBM personal computers. Purchase of these computers was justified on the basis of the benefits of spreadsheet analysis, data storage and retrieval, output presentation, reduced keying, and faster turnaround of special projects. By 1984, a proposal had been developed to place a workstation on the desk of every individual within BS&R and to establish a LAN that could be used to pass documents, send and receive messages, and communicate with other workstations as well as with the Board's mainframe. After evaluating alternative token-ring network operating systems available in 1989, SIR staff selected Novell NetWare because they determined that it had a dominant presence in the market, superior performance for the type of analysis and processing done in BS&R, and strong security features. Since then, SIR's automation efforts have emphasized expanding services on the network; upgrading

Figure 1
**Supervisory Information Resources Organization Chart**

```
                    ┌──────────────────┐
                    │    Assistant     │
                    │     Director     │
                    │    (Vacant)      │
                    └──────────────────┘
                             │
                    ┌──────────────────┐
                    │     Manager      │
                    │ Supervisory Info │
                    │    Resources     │
                    └──────────────────┘
                             │
        ┌────────────────────┼────────────────────┐
┌─────────────────┐ ┌─────────────────┐ ┌─────────────────┐
│ Senior IS Analyst│ │Senior IS Analyst│ │Senior IS Analyst│
│   Help Desk     │ │  Applications   │ │    Network      │
│                 │ │                 │ │ Administration  │
└─────────────────┘ └─────────────────┘ └─────────────────┘
```

 workstations; adding client–server capabilities to support the growth in database applications; connecting BS&R to the Records Management System in the Office of the Secretary; and promoting BS&R's use of the Windows NT operating system and the standard application product suite, consistent with AD 96-39.

Current BS&R Distributed Processing Environment

As figure 2 illustrates, BS&R's Novell NetWare operating system supports a network of more than 250 workstations and 35 laser network printers interconnected across two Washington, D.C., office locations (the Martin and New York Avenue buildings). The network supports more than 30 different distributed software products, including word processing, spreadsheet, database, and graphics packages. Through the Board's wide area network, users also have access to services such as electronic mail, the Internet, database and document management systems, a CD-Rom server, and dial-in and dial-out capabilities.

Figure 2
High Level Diagram of BS&R's Distributed Processing Network
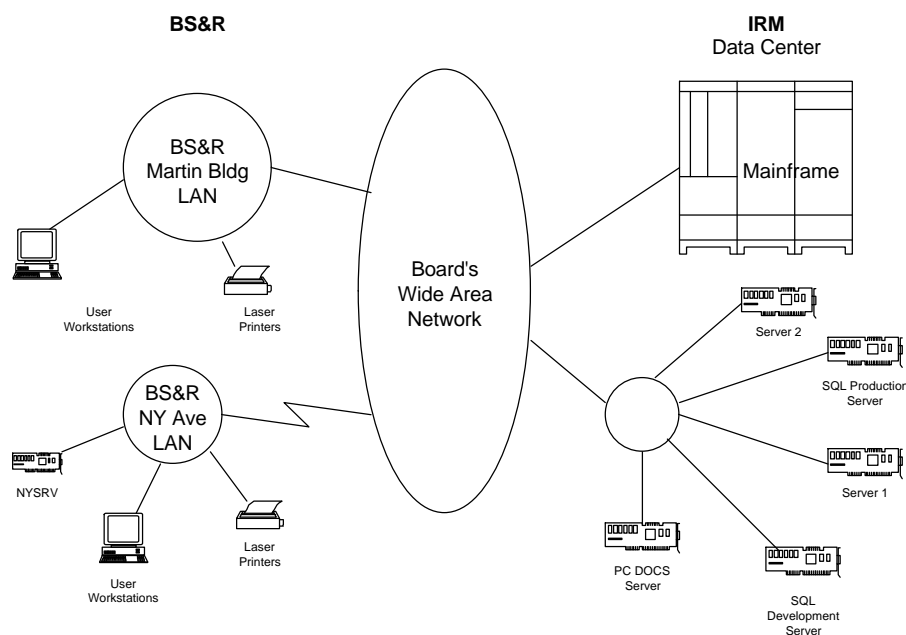
OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted audit fieldwork from November 1996 to January 1997. Our audit objectives were to determine if BS&R has (1) established an effective process for planning, organizing, directing, and controlling the activities related to distributed processing, (2) adequately managed the efficiency of its LAN and developed an effective problem management system, (3) properly secured its distributed systems and data, and (4) developed appropriate backup and disaster recovery procedures.

While we obtained a high-level perspective of the S&R function's strategic plan and overall organization for handling information technology issues, our audit focused on activities SIR performed and the related support IRM provided. We evaluated network access and security functions provided by Novell NetWare. We did not evaluate the users' control over specific applications or data, or the methodology used to develop applications processed on the network. Because BS&R was just beginning to migrate to the Windows NT operating system, we performed a high–level review only of how Windows NT interfaces with Novell NetWare in authorizing and controlling access to applications.

To accomplish our audit objectives, we reviewed policies, procedures, and related documentation; interviewed Board staff; and performed various tests. Specifically, we reviewed automation strategic plans, the system configuration diagram, problem tracking logs, various system security reports, and BS&R's draft contingency plan. We interviewed the Deputy Director of BS&R, SIR management and staff, the Director of IRM, and members of IRM staff who interact with SIR to support BS&R's LAN. To gain a general understanding of user perceptions regarding BS&R distributed processing, we sent out an office automation survey to 240 BS&R LAN users and received 151 responses. After analyzing the survey results, we provided a summary of the results to BS&R management. We also tested problem log entries by selecting a sample of the problems logged during December 1996 and contacted the users to discuss their experience. Finally, we selected a sample of workstations to observe physical security and to discuss logical security, virus protection, installed software, and backup procedures with the users. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, we found that BS&R has adequately managed its distributed processing environment. BS&R's *Strategic Office Automation Plan*, which SIR had prepared to cover the 1995 through 1997 time frame, identified major objectives that were consistent with Systemwide initiatives and helped to guide SIR in maintaining a high level of system performance. BS&R managers and staff who responded to our user survey were generally satisfied with the availability of applications on the LAN and the daily reliability of the LAN. About 82 percent of the respondents indicated that they "seldom" or "never" experienced technical problems in accessing or using applications.

BS&R has also taken steps to develop appropriate backup and disaster recovery procedures and to build an effective problem management system for LAN users. Using the software that the Board purchased to develop division and Boardwide business resumption plans, SIR developed a disaster recovery plan which it plans to test in the near future. Additionally, SIR recently developed an automated problem log database to track user calls to the help desk.

Notwithstanding these accomplishments, we are concerned about BS&R's ability to effectively and efficiently meet the distributed processing challenges that are and will be facing the division and the Systemwide S&R function. Specifically, we believe that having a vacant Assistant director position over an extended period hampers SIR's ability to

— prepare a strategic office automation plan for the 1998 to 2000 planning period that is consistent with the strategic direction of the S&R function Systemwide;

— actively participate in the technology decision making process; and

— develop practical, comprehensive plans for making an orderly migration to the new operating system and product suite within established milestones, including ensuring sufficient expertise.

In addition, though security over the existing LAN is generally adequate, we found opportunities to strengthen controls by implementing additional security features. As BS&R implements a dual network operating system environment, we believe SIR needs to examine Windows NT security capabilities closely and evaluate options that would optimize overall distributed processing controls, including possibly eliminating Novell Netware. Finally, we believe that formalizing policies and procedures could improve communications and strengthen network management and control as BS&R migrates to the new operating system platform at the workstation level and that implementing more formal procedures would help ensure that problems are consistently resolved in a timely manner.

Our first two recommendations are intended to strengthen SIR leadership, ensure that BS&R's distributed processing environment is operating with a strategic vision that is consistent with that of the S&R function, and provide for an orderly transition to the new operating system and product suite. Recommendation three is intended to improve security controls in both the Novell NetWare and Windows NT operating systems. Although BS&R's current Novell Netware operating system configuration generally provides adequate security over the network, we found nine vulnerabilities that indicate that security controls need to be enhanced. We have provided these technical findings, along with specific recommendations for corrective action, under a separate restricted cover to the Deputy Director of BS&R for appropriate disposition. Recommendation four addresses the need to define and implement formal policies and procedures for both users and system administrators. Finally, recommendation five is intended to strengthen the help desk problem tracking and resolution process.

1.   We recommend that the Director of BS&R implement an organizational structure that will provide strategic leadership for distributed processing in the division and ensure appropriate liaison on S&R information technology issues that are addressed across the System.

BS&R needs strong, sustained, and visible leadership and a logical organizational structure to manage successfully its internal distributed processing environment and participate proactively in the strategic decision-making process for acquiring and using automation, communication, and information technology across the S&R function. BS&R looks to SIR to manage the operation and growth of BS&R's divisionwide office automation systems and to prepare BS&R's strategic office automation plan. At the division level, SIR's distributed processing objectives must be driven by division users and their business processes as well as by Board technology strategies and automation platforms. At the System level, SIR's distributed processing objectives must be properly aligned with the strategic direction that information technology is taking across the S&R function, so that BS&R can adopt new and emerging technologies in a timely, effective manner.

Having an organizational framework that enables SIR to work in concert with these various business and technology requirements is particularly important as BS&R and the System develop the new strategic plans that will carry the S&R function into the next century.

Though BS&R has been well represented in S&R information technology discussions from a business process perspective, representation from the technical automation perspective has been lacking. Having a vacancy at the Assistant director level since September 1995 may be limiting SIR's involvement in key Systemwide distributed processing issues that directly and substantively affect BS&R. Before his departure, the Assistant Director of SIR had been a member of the Automation Working Group and the S&R Automation Strategic Planning Group that supported the Automation Oversight Committee, the predecessor of the ITC. Since his departure, however, SIR has not been represented on the ITC and has not had the organizational framework it needs to participate in the technology decision-making process or to prepare fully for implementing Windows NT and Microsoft Office in BS&R along with the rest of the System.

Because SIR is not directly involved in the key strategic decisions that affect its mission and responsibilities, SIR staff typically must operate reactively in preparing for and implementing key decisions. Although SIR is responsible for developing the new strategic office automation plan that will carry BS&R into the year 2000, it lacks the Systemwide strategic vision necessary to accomplish this task. The lengthy delay in filling the assistant director position has also contributed to a certain level of frustration among the staff, even though BS&R top management have reassured them periodically that organizational issues were being carefully considered and would eventually be addressed.

BS&R's senior management is very aware of the System's information technology initiatives and realizes that the division's current organization structure does not give SIR the prominence needed to address technology issues strategically or to deal effectively with competing priorities. The Deputy Director of BS&R told us that a reorganization of the division is being considered and that it should better position the division to provide strategic leadership for its internal distributed processing environment and ensure appropriate liaison on both system and division S&R information technology issues.

2.   **We recommend that the Director of BS&R ensure that the plan to implement Windows NT and Microsoft Office specifically addresses security, training, and administration for both network administrators and users.**

A practical, well-organized plan is critical to manage effectively the many technical, security, and administrative issues associated with implementing a new operating system and replacing diverse application tools with a standard application product suite. Effective planning involves many tasks: establishing clear goals and milestones for migrating to the new technology; ensuring that network administrators and other technical staff receive appropriate training on the system configuration and use; outlining the steps needed in setting up the system infrastructure (e.g.,

hardware, network tuning, etc.); designing and testing key system interfaces; documenting procedures for primary business operations; and training end users in how to use the operating system and product suite to their full potential. Such a plan is particularly important when the organization responsible for leading the technology implementation has had limited direct involvement in the process leading up to the standardization decision (see recommendation 1, page 7).

SIR has already taken some steps in preparing for the migration. For example, it purchased software licenses for Windows NT and Microsoft Office and is working to ensure that its hardware is at the recommended level for implementing the new operating system. SIR has also prepared a draft plan that lays out a schedule for upgrading each section within BS&R to Windows NT and Microsoft Office. To handle the Windows NT upgrade, the SIR manager has established a task force that is working to resolve technical issues, identify training, and prepare documentation to assist in the transition.

We support these efforts, but we believe that much remains to be done to effectively meet the migration time frames established in AD 96-39. The plan to migrate the 240 users in the division to the new operating environment is just being developed, even though the division is supposed to convert to Windows NT effective July 1, 1997, and to Microsoft Office effective January 1, 1998. SIR hired a new network administrator with Windows NT expertise in February 1997, which should prove invaluable in the migration effort. However, the other individuals in SIR who are responsible for network administration have limited knowledge about the capabilities and security requirements for Windows NT and, at the time of our review, had not yet received training to build their expertise. A communication plan to inform and prepare the users for the transition has not yet been prepared. Several comments in response to our survey indicated that communication about software upgrades and changes need to be improved. In addition, users had not been scheduled for training on Windows NT or Microsoft Office. Finally, policies and procedures for administering and using the new operating environment and software application have not yet been prepared.

We believe that more in-depth planning will help make BS&R's migration to the new software successful. A solid implementation plan would also enhance BS&R's ability to work more effectively with the Reserve Banks as they also move to the S&R function's standard operating environment.

3. **We recommend that the Director of BS&R improve security controls over BS&R's distributed processing environment by evaluating and appropriately implementing the security capabilities of Novell NetWare and Windows NT to ensure that they comply with the *Information Security Manual*.**

Network operating systems such as Novell NetWare and Windows NT control the operation of the computing and communications equipment under which software applications are developed

and executed. These operating systems have a variety of "option settings" that allow network administrators to tailor and customize system security. For example, Novell NetWare's option settings control and monitor system software features that can be set to allow supervisor access to all system resources, restrict the resources a user may access and the types of accesses that are allowed, and maintain the integrity of the user log–on process. Inappropriate settings create unnecessary security exposures and could cause the division to be out of compliance with the minimal security requirements of the *Information Security Manual*.

BS&R's current Novell NetWare operating system configuration generally provides adequate security over the network; nevertheless, we believe implementing additional security features would strengthen controls. In reviewing of BS&R's Novell NetWare operating system we detected nine vulnerabilities that indicate that security controls need to be enhanced in four areas:

1.   consistent implementation of access controls (i.e, passwords);

2.   separation of the duties of users and programmers;

3.   implementation of virus protection controls; and

4.   use of compensating and complementary controls.

The detailed technical findings and recommendations for corrective action in each of these areas have been reported under separate restricted cover to the Director of BS&R.

Although a detailed review of the Windows NT operating system was outside the scope of our audit, we did conduct a limited review of the interface between Windows NT and Novell NetWare in controlling access to important BS&R databases like FRED. The new file manage-ment system available on Windows NT offers enhanced reliability and data security and should be used in conjunction with, or possibly replace, Novell NetWare's security features to optimize BS&R's overall security controls. For example, enabling available Windows NT security features for FRED would strengthen the limited network security controls that are now in place to protect sensitive data. By closely examining and properly implementing both the Novell NetWare and Windows NT security capabilities, BS&R will be better able to ensure that the division meets the minimum requirements of the *Information Security Manual*, fully capitalizes on the available technical capabilities of the operating systems, and avoids exposure to unnecessary risks.

4.   We recommend that the Director of BS&R define and implement policies and procedures for using and administering distributed processing in the division, as part of the migration to the new technology platform.

Our review of BS&R's existing policies and procedures for distributed processing found that the division has well-documented application development standards and a comprehensive disaster

recovery plan. However, we did not find comprehensive distributed processing policies and procedures for either users or technical staff. We also found that users were not always knowledgeable of their responsibilities with regard to backup, virus scan protection, and problem reporting.

Technical and user policies and procedures for distributed processing should be documented and kept up to date, regardless of the network operating system used. Lack of adequate documentation to describe programs, hardware, system configuration, and procedures may result in the inability to use or support the system, or to recover from problems. Without formal policies and procedures, users may not understand their responsibilities and it will be difficult to hold them accountable for implementing proper controls. Additionally, formal policies and procedures facilitate system administration and ensure continuity of system operations in case of the loss of key technical personnel.

We believe opportunities exist to improve communications and strengthen controls by formalizing policies and procedures as the division migrates to the new technology platform. Specifically, user policies and procedures should be documented for the key areas such as virus scan protection, logging on and off the system, problem reporting, hard drive backup, personal software, copyright policy, and purchasing new hardware and software. Additionally, system administration policies and procedures should be documented for the areas of security, backup, service-level agreements, standard workstation configuration, and problem resolution. SIR recognizes the value of documentation and believes that the Board's FedWeb system will prove beneficial in distributing new documentation and ensuring that it stays up to date.[4]

5.   **We recommend that the Director of BS&R strengthen the help desk problem tracking and resolution process by establishing formal procedures to rank problem severity, assign resolution deadlines, follow up on problem status, communicate problem status to users, and implement periodic management review and trend analysis of problems**.

The help desk and the problem reporting, tracking, and resolution process are important components of network management and control. Some typical activities associated with a user help desk include receiving and recording all user problem calls, validating user procedures, updating problem records to track all unresolved problems, and giving users problem status updates. In our opinion, both the help desk function and the problem management process can be invaluable in maintaining user productivity. Lack of formal problem management procedures could lead to inefficient processes, unresolved errors, potential risk exposures, and user dissatisfaction and lack of confidence in the system.

---

[4]FedWeb is a Federal Reserve Systemwide Intranet, based on Internet technologies such as the World Wide Web, that allows the sharing of information among the System's organizations.

SIR has recently developed a help desk database application to log user problems and provide a detailed problem record of all calls to the help desk. Each problem record includes a field for the date the problem was opened, a description of the problem, the diagnosis, the analyst assigned the problem, its priority, the status of the problem, the resolution, and the close date. The help desk application also provides status reports and statistical reports that classify problems in categories such as hardware problems, network, new users, relocation, and software problems. Although the help desk database application is comprehensive, we found that the problem resolution process is generally informal.

Information gathered from users in our office automation survey and during testing was both positive and negative with regard to the help desk. Overall, responses to the user survey indicated that technical problems arise rather infrequently, but 22 percent were dissatisfied with the process for resolving problems once they did occur. The individual comments further expanded on this statistic, with respondents commenting that they felt that the help desk needed to respond more promptly and implement a follow-up procedure to make sure that a problem was attended to or resolved. We tested a sample of eight of the 114 problems logged during December 1996 by contacting the users to discuss their experiences. Most were satisfied with the response they received, although one expressed concern over the help desk's delay in either correcting the problem or following up on the status of the problem resolution effort.

We believe opportunities exist to improve the help desk service level and enhance "customer service" by implementing more formal help desk procedures. Specifically, we believe formal procedures are needed to standardize entering of data in the problem log, categorizing and prioritizing problem severity, adding a projected resolution "need by" date to the problem log data base, following up on problem status, communicating problem status to the users involved, and requiring periodic management review of the problem log status and analysis of problem trends.

ANALYSIS OF COMMENTS

The Deputy Director of BS&R's response to our draft report indicates general agreement with the five recommendations (see appendix 1). Specifically, he states that senior division staff has developed a plan to restructure the divisions's organization to provide additional strategic leadership for distributed processing in the System and the division; includes a detailed plan that specifically addresses security, training, and procedures for implementing Windows NT and Microsoft Office in the division; describes steps that have been taken to address the specific security vulnerabilities noted in our separate management letter; states that distributed processing policies and procedures will be prepared; and indicates that help desk procedures will be formalized.

APPENDIXES

Appendix 1 - Division's Comments

Date:	June 4, 1997
To:	Barry R. Snyder
From:	Stephen C. Schemering *ALN*
Subject:	Comments on the Draft Report on the Audit of the Division of Banking Supervision and Regulation's Distributed Processing Computing Environment (A9610)

Enclosed are my comments on the Inspector General's draft report on the Operations Review Report of the Division of Banking Supervision and Regulation. I view the report as providing a generally fair assessment of the Division and agree with the Report's summary of findings and recommendations. The Division concurs in full with all recommendations. We have implemented or have plans to implement policies, procedures and practices in response to the following recommendations:

I.   We recommend that the Director of BS&R implement an organizational structure that will provide strategic leadership for distributed processing in the division and ensure appropriate liaison on S&R information technology key issues being addressed across the System.

Concur. Senior division staff has developed a plan to restructure the division's organization. Once approved and implemented the plan will provide additional strategic leadership for distributed processing in the division and appropriate liaison on key information technology issues being addressed across the system.

II.   We recommend that the Director of BS&R ensure that its plan for implementing Windows NT and Microsoft Office specifically addresses security, training, and administration for both network administrators and users.

A.   The Plan - Implementation of Windows NT and MS Office

At the June 1996 Conference of the Officers in Charge of Supervision decisions were made as to software standards and migration time frames for the supervision function. Specifically, two software standards were developed:

(1) Effective July 1, 1997 the supervision functions's desktop PC operating system standard will be Windows 95/Windows NT. Portable PCS should be equipped with Windows 95.

(2) Effective January 1, 1998, the supervision function's software application standard will be

Appendix 1 - Division's Comments

Microsoft Office 95

The proposed plan is to install the Windows NT 32-bit operating system and Microsoft Office 95 or its successor on 223 desktop PCS before July 1, 1997. The Supervisory Information Resources section has installed over 100 Microsoft Office Professional Suites (v.4.3) for Windows 3.1 workstations. This software will migrate into the Windows NT environment without loss of current capability. We are confident that Microsoft Office 95's successor Office 97 will be installed throughout the Division before January 1, 1998. We have also completed a thorough test of Windows NT, identified some of its limitations and will install a work-around to address these limitations.

Our plan for each section includes:
(1) A review of all automation resources currently installed,
(2) A discussion with the section manager of all documented requests for upgrades to hardware or software,
(3) A description of the schedule and all upgrades for that section.
(4) A discussion of the preparation the section staff will be required to make in order to expedite the installation of new hardware and software,
(5) An explanation of the brief orientation and documentation that all members of the staff. will be given after each PC is upgraded,
(6) An announcement and an explanation of the objectives of the brief introductory classes conducted in the IRM educational center or in BS&R for division staff.

All PC hardware, operating systems, and the installation of Microsoft Office software have been installed in the SIR, International Supervision, International Regulations, International Applications and the Regulatory Reporting and Accounting Issues sections. The following schedule lists the start dates for all sections:

START DATE-1997	SECTION
3/10	Supervisory Info Res
3/13	Administration
3/17	International Supervision
3/27	International Reg/Exam Policy
4/1	International Applications
4/4	Reg Rep/Acct Issues
4/25	Training
5/1	NIC Function Office
5/5	Surveillance
5/8	Regional/Community
5/14	Multinational
5/20	Financial Analysis
5/26	Trust
5/28	Applications Analysis

Appendix 1 - Division's Comments

6/3	**Enforcement**
6/5	**Special Investigation**
6/10	**Supervisory Rev/Eval**
6/12	**Policy Development**
6/17	**Policy Implementation**
6/23	**Securities Regulation**
6/25	**Application Issues**
6/30	**Program Direction**

SIR staff will perform the upgrades, which will include **(a)** upgrading the PC hardware to at least a Dell 486/66 if required, **(b)** installing Microsoft Office, **(c)** installing the Windows NT operating system, and **(d)** mapping over all data files from the old PC. All Division staff members will be asked to cooperate with the SIR section during a very demanding transition.

B.   **Security** - All procedures and safeguards required by the "Information Security Manual" (ISM) and the "Distributed Processing Support Manual" have been complied with by user support staff, network administrators and users for installing, operating and maintaining the current Windows/DOS desk top and the Novell NetWare network operating system. We will continue to enforce these procedures and safeguards. The NT installation team, with the assistance of other analysts in the SIR section, the division security officer and the information security committee will continue to analyze the NT operating system for inconsistences that could present new threats to the security and integrity of division electronic information. The result of this research will be used to provide additional security for data and other information. The primary procedure that network administrators and analysts will continue to perform to insure that inconsistences in new PC operating systems do not threaten the security of our data is the ISM risk assessment. If new threats are identified, the current information security channels of communication and education would be used to inform users of changes to their normal operating procedures in order to comply with the ISM.

C.   **Training** - division network administrators, members of the user support group and members of the application development group have attended the "Introduction to NT 3.51" classes conducted in the IRM education center, as well as introductions to Micro Soft Office Suite classes. The recently hired information system analyst, who is responsible for providing network operation and analytic support, successfully implemented and operated NT networks for the State Department. The SIR section will continue to attend all internal classes on the installation and maintenance of NT based desk top PC's or NT based networks. Upon the completion of the installation of NT based software on the user's desk top PC, the installer explains to the the user the differences between operating their old work station and their new NT work station and gives the user a 15 page NT Primer/User guide. The user is also informed of a one day NT introductory class that was designed for BS&R staff. We also are encouraging all section managers to **provide other training opportunities**, especially those that explain how to use the enhanced processing features of 32-bit applications.

Appendix 1 - Division's Comments

D.   Administration - all procedures required to install, maintain, and operate NT work stations, as well as those procedures required to administer and operate a network that supports PC's with NT operating systems are being documented and modified for operation in the BS&R automation environment as we gain experience with the transition from Windows/DOS. Some of the sources of information used to generate administrative and user guidelines are reference documents from classes given outside of the Board as well as internal Board classes.

III.   We recommend that the Director of BS&R improve security controls over BS&R's distributed processing environment by evaluating and appropriately implementing the security capabilities of Novell NetWare and Windows NT to ensure that they comply with the *Information Security Manual.*

Concur: Prior to the Inspector General's review, this division was in the process of implementing or had plans to implement procedures responsive to this recommendation. These procedures will be fully applied, documented and monitored.

IV.   We recommend that the Director of BS&R define and implement policies and procedures for using and administering distributed processing in the division.

Concur. Recommendation will be implemented as follows:

A.   A manual will be prepared to define division policies and procedures for using distributed processing (dp). Management and the staff will be asked to identify information that they would find useful. This information will cover a wide range of interests and needs and will at a minimum cover the following topics:

1)   Documentation and an explanation of current IRM and BS&R dp topology
2)   Explain why dp policies and procedures are necessary
3)   Data access authorization
4)   The purpose and use of the ISM
5)   The help desk and how to use it
6)   The staff's responsibility for protecting the data on their PC
7)   How to back up your PC
8)   How to request automation resources

B.   Documentation will be prepared to define division policies and procedures for administering distributed processing. This information will at a minimum include the following topics:

1)   Procedures for performing network administration
2)   Procedures for providing help desk user support
3)   Procedures for developing desk top applications
4)   Procedures for administering access request applications

(A9610)   20

Appendix 1 - Division's Comments

5) A description of HRM new employee orientation
6) How to coordinate and facilitate communication between users and service providers
7) Explain SIR's responsibility for applying ISM policies and procedures.
8) Explain the necessity for policy and procedures for administering dp
9) How to contribute to strategic planning, budgeting, allocating and maintaining dp resources
10) SIR's network group policies and procedures that aid:
   - system and desk top backup
   - service level agreements and subscriptions
   - software inventory and license control
11) SIR's user support group policies and procedures that aid:
   - standardization of work station configurations
   - software installation using network based programs
   - user problem resolution

V.   We recommend that the Director of BS&R strengthen the help desk problem tracking and resolution process by implementing formal procedures to prioritize problem severity, assign resolution deadlines, follow-up on problem status, communicate problem status to users, and implement periodic management review and trend analysis of problems.

Concur   Recommendation accepted and is being implemented as stated. The recommendation will be fully implemented during the fourth quarter of 1997. At this time new help desk operation procedures as well as current procedures are being reviewed. We will discuss several alternatives for evaluating the organization of the user support group as well as the management of the user support group. Modifications to the help desk database programs are being discussed in order to develop automated procedures to prioritize user problem severity and to force a documented commitment to a resolution schedule or deadline. It is expected that the division's restructuring of it organization will make it easier to reassign some of the tasks in the SIR section in order to assign someone on a full time basis to follow up on problems status as well as communicating the current status to users. This individual will also be asked to assure that user problems are prioritized and that resolution deadlines are assigned and followed. Using the IG's survey format and modifying some of the questions asked we expect to perform more timely and informative trend analysis of user problems and the response of the SIR help desk user support group. With this information, division management will be prepared to make the necessary adjustments to the operation of the help desk.

Appendix 2 - Principal OIG Contributors to this Report

▸   Bonnie Smolak, Senior EDP Auditor and Auditor-in-Charge

▸   Beth Coleman, Senior Auditor

▸   Gary Lester, Senior EDP Auditor

▸   Pam Debnam, Senior Secretary

▸   Patty Kelley, Audit Manager